



(19) Europäisches Patentamt
European Patent Office
Office européen des brevets



(11) EP 1 051 009 A1

(12)

DEMANDE DE BREVET EUROPEEN

(43) Date de publication:
08.11.2000 Bulletin 2000/45

(51) Int Cl? H04L 29/06, G06F 1/00

(21) Numéro de dépôt: 00401161.5

(22) Date de dépôt: 27.04.2000

(84) Etats contractants désignés:
AT BE CH CY DE DK ES FI FR GB GR IE IT LI LU
MC NL PT SE
Etats d'extension désignés:
AL LT LV MK RO SI

(30) Priorité: 06.05.1999 FR 9905763

(71) Demandeur: ALCATEL
75008 Paris (FR)

(72) Inventeurs:
• Marquet, Bertrand
92160 Antony (FR)

• Fouquet, Guy
91620 Nozay (FR)
• Ballester, Laurent
78700 Conflans Sainte Honorine (FR)

(74) Mandataire: Lamoureux, Bernard
COMPAGNIE FINANCIERE ALCATEL
Dépt. Propriété Industrielle
30, avenue Kléber
75116 Paris (FR)

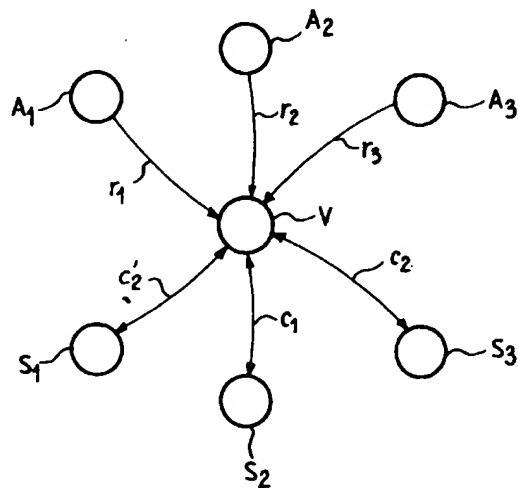
(54) Serveur virtuel fournissant des services de sécurité

(57) Serveur virtuel de sécurité permettant à un ensemble d'applications d'accéder à un ensemble de services de sécurité, caractérisé en ce qu'il possède :

- des moyens pour recevoir de la part des applications logicielles des requêtes de services,
- des moyens de communication avec des serveurs

de sécurité mettant en œuvre ces services de sécurité,
des moyens pour choisir au moins un serveur de sécurité destinataire pour chaque requête de service reçue et pour lui transmettre des informations lui permettant de fournir le service de sécurité correspondant à la requête de service.

FIG_2



Description

[0001] La présente invention est relative à un système informatique nécessitant la sécurisation des communications entre certains des composants logiciels le composant.

[0002] L'invention s'applique particulièrement bien aux systèmes de gestion de réseau, notamment de réseau de télécommunication. Cet exemple d'application sera plus particulièrement développé par la suite, mais l'invention est toutefois susceptible de s'appliquer à d'autres types d'applications, par exemple aux applications pour le commerce électronique.

[0003] De façon classique, les systèmes de gestion de réseaux de télécommunication comportent un ensemble d'applications logicielles de gestion. Ces applications peuvent être réparties au sein d'un système distribué, et peuvent avoir besoin de communiquer entre elles afin d'échanger des informations.

[0004] Un besoin peut exister de sécuriser ces communications. En fonction de la menace que l'on craint ainsi que du niveau de sensibilité des informations transmises, différents services de sécurisation peuvent être mis en œuvre, comme par exemple :

- Identification et authentification : par cette technique, le destinataire d'un message est assuré de l'origine de ce message. On a ainsi la garantie qu'il n'existe pas de messages émis par un tiers malveillant dans le système.
- Contrôle d'accès : une application ne réagira aux commandes contenues dans les messages, qu'en fonction de règles définies dans une politique de sécurité. Par exemple, une application peut ne communiquer qu'avec un ensemble déterminé de correspondants.
- Non-répudiation : un certain nombre d'informations sur les messages échangés sont mémorisées afin qu'aucune des parties prenantes ne puisse renier le fait d'avoir participer à la communication.
- Confidentialité : les messages sont chiffrés de sorte qu'un tiers ne puisse être en mesure d'en interpréter le contenu.

[0005] Typiquement, ces services, ainsi que d'autres non mentionnés, sont mis en œuvre par des applications logicielles spécifiques que l'on appelle serveurs de sécurité. Plusieurs serveurs de sécurité peuvent exister, chacun fournissant un ou plusieurs des services de sécurisation. De même chaque service de sécurisation peut être fourni à différents niveaux de qualité.

[0006] La figure 1 présente une architecture conforme à l'état de la technique dans ce domaine. L'application A₁ souhaite sécuriser une communication avec l'application A₂. Pour cela, elle peut utiliser le serveur de sécurité S₁ qui fournit un support bas-niveau de cryptographie, ou bien le serveur de sécurité S₂ qui fournit un service de cryptographie de haut-niveau.

[0007] Dans le cas où l'application A₁ utilise le serveur S₁, elle envoie dans un premier temps un message m₁ de requête de service au serveur S₁. Ce serveur S₁ retourne une clé dans un message de réponse m₂. Ensuite, l'application A₁ peut envoyer son message m₃ à destination de l'application A₂ après l'avoir chiffré avec la clé.

[0008] Dans le cas où l'application A₁ fait appel au serveur de sécurité S₂, elle confie son message à transmettre m₁ au serveur de sécurité S₂. Ce serveur S₂ se charge alors de mettre en œuvre les techniques de cryptographie puis transmet le message crypté m₂' à l'application destinatrice A₂.

[0009] Ces deux exemples triviaux permettent de mettre en exergue le fait que pour un même service de sécurisation, différents niveaux de services peuvent être disponibles. De la même façon pour un même service et un même niveau de service, il peut exister différents protocoles de négociation entre l'application initiatrice (A₁) et le serveur de sécurité. C'est par exemple le cas pour la négociation de la clé de chiffrement dans le cas d'un service de cryptographie. On peut citer, à titre d'exemples de tels protocoles, les méthodes de Diffie-Hellman ou de Needham-Schröder. Ces méthodes sont par exemples présentées dans l'ouvrage intitulé "Practical Intranet Security" de Paul Ashley et Mark Vandenwauver, publié aux éditions Kluwer Academic Publishers en 1999.

[0010] Pour résumer, une application désirant sécuriser une communication avec une autre application, devra être capable de mettre en œuvre différents protocoles de négociation en fonction du service et du niveau de service qu'elle désire.

[0011] Cela implique aussi que si l'on désire remplacer un serveur de sécurité correspondant à un service et un niveau de service donné, par un autre présentant par exemple une meilleure qualité de service mais mettant en œuvre un protocole de négociation différent, les applications devront être modifiées si elles n'étaient pas prévues dès le départ pour ce nouveau protocole.

[0012] De plus, les moyens de communication à utiliser pour atteindre chacun des serveurs de sécurité peuvent être différents. Par exemple, chacune des applications doit donc pouvoir gérer un accès direct, ou à travers un bus logiciel comme CORBA (*Common Object Request Broker Architecture*) de l'OMG (*Open Management Group*) ou DCOM (*Distributed Common Object Management*) de la société Microsoft, ou encore à travers un réseau.

[0013] Le but de la présente invention est, entre autres, de pallier ces différents inconvenients. Pour cela, elle a pour objet un serveur virtuel de sécurité permettant à un ensemble d'applications logicielles d'accéder à un ensemble de services de sécurité. Ce serveur virtuel de sécurité se caractérise en ce qu'il possède :

- des moyens pour recevoir de la part des applications logicielles, des requêtes de services,

- des moyens de communication avec des serveurs de mettant en oeuvre les services de sécurité en question,
- des moyens pour choisir au moins un serveur de sécurité destinataire pour chaque requête de service reçue et pour lui transmettre, via ces moyens de communication, des informations lui permettant de fournir le service de sécurité correspondant à la requête de service, certaines au moins de ces informations étant contenues dans la requête de service.

[0014] Selon une mise en oeuvre de l'invention, les applications logicielles peuvent accéder au serveur virtuel de sécurité au travers d'une interface de programmation ou API (pour *Application Programming Interface*, en anglais).

[0015] Selon une mise en oeuvre de l'invention, le serveur virtuel de sécurité peut être développé en un langage de programmation tel Java.

[0016] L'invention a aussi pour objet le procédé susceptible d'être mis en oeuvre par les applications logicielles pour utiliser ce serveur virtuel de sécurité. Ce procédé se caractérise en ce qu'il comporte les étapes de :

- émission de requêtes de service par une application logicielle à destination d'un serveur virtuel de sécurité,
- choix, par le serveur virtuel de sécurité, d'un serveur de sécurité destinataire, à même de fournir le service de sécurité correspondant à cette requête de service,
- émission d'informations à destination du serveur de sécurité destinataire afin qu'il puisse fournir le service de sécurité, certaines au moins de ces informations étant contenues dans la requête de service.

[0017] La figure 1, déjà commentée, représente une architecture conforme à l'état de l'art permettant la sécurisation de communications entre applications.

[0018] La figure 2 représente une architecture générale conforme à l'invention.

[0019] La figure 2 schématisé un exemple d'architecture conforme à l'invention. Les références A₁, A₂ et A₃ représentent trois applications logicielles. Ces applications peuvent émettre trois requêtes de service, r₁, r₂ et r₃ respectivement, au serveur virtuel de sécurité V afin de sécuriser les communications qu'elles désirent initier.

[0020] Selon une mise en oeuvre de l'invention, ces requêtes contiennent uniquement le type de services désiré (confidentialité, authentification...).

[0021] Le serveur virtuel de sécurité a alors pour tâche de déterminer le ou les serveurs de sécurités parmi l'ensemble disponible S₁, S₂ et S₃, qui permettent de fournir le service demandé. Pour cela, le serveur virtuel

V peut posséder un moyen de mémorisation permettant d'associer les services de sécurité demandés par les applications et les serveurs de sécurité fournissant ces services.

5 **[0022]** Dans l'exemple de la figure 1, la requête de service r₁ engendre une requête c₁ entre le serveur virtuel V et le serveur de sécurité S₂. Cette requête peut être composée d'un échange de messages entre les deux participants. Cet échange dépend du serveur de sécurité S₂ et du protocole de négociation qu'il met en oeuvre. On voit que cette architecture masque le protocole de négociation en question pour l'application qui n'a donc pas besoin de s'en préoccuper.

[0023] Par ailleurs l'application A₂ émet au serveur virtuel de sécurité V une requête de service r₂. Cette requête va être interprétée par le serveur virtuel de la même façon que précédemment, mais ici la réalisation du service demandé nécessite deux serveurs de sécurité, S₁ et S₃, avec lesquels le serveur virtuel initie deux requêtes c₂ et c'₂.

[0024] Selon l'architecture conforme à l'invention, les applications (A₁, A₂ et A₃) peuvent n'avoir aucune information sur les différents serveurs de sécurités (S₁, S₂, S₃). Comme évoqué précédemment, cela simplifie les communications entre les applications puisque celles-ci sont déchargées de la gestion des différents protocoles de négociation, ainsi que du choix du ou des serveurs de sécurité appropriés au service requis. Il résulte de cela une simplification du développement des applications, et donc une réduction du coût associé.

[0025] Par ailleurs, il est courant d'ajouter un serveur de sécurité au sein d'un système de gestion de réseaux, ou d'en remplacer un par un autre. Dans une architecture selon l'état de l'art, cet ajout ou ce remplacement peut résulter sur un nouveau protocole à prendre en compte par les applications, ou en tout cas par un nouveau serveur à prendre en compte pour remplir les services de sécurité pouvant être requis. Cela implique donc nécessairement la modification de toutes les applications concernées.

[0026] Au contraire, dans une architecture selon l'invention, seul le serveur virtuel doit être adapté. Bien évidemment, le coût engendré par la modification d'un unique composant logiciel bien identifié est bien moindre que celui qui serait nécessaire pour modifier tout un ensemble de composants logiciels hétérogènes.

[0027] De plus, l'architecture selon l'invention permet l'utilisation de plusieurs serveurs de sécurité pour réaliser un même service de sécurité. Cette utilisation est totalement transparente pour les applications. Il est ainsi aisément possible de rendre disponibles des services de sécurité de haut niveau, et de tirer profit des capacités des serveurs de sécurité pour rendre un service qu'ils ne peuvent pas offrir individuellement.

[0028] Par ailleurs, c'est au serveur virtuel que revient la charge de gérer la localisation physique des différents serveurs de sécurité ainsi que le moyen d'accès correspondant : accès direct ou par un bus logiciel par

exemple.

[0029] Enfin, les applications peuvent n'avoir aucune information sur les serveurs de sécurité autres que le serveur virtuel V. Par conséquent, elles peuvent n'avoir aucune information sur les protocoles de négociation mis en oeuvre, et les attaques malveillantes du système n'en seront que plus difficiles.

[0030] Selon une mise en oeuvre de l'invention, les applications logicielles peuvent accéder aux fonctions du serveur virtuel au travers d'une interface de programmation ou API (Application Programming Interface).

[0031] Selon une mise en oeuvre particulière de l'invention, le serveur virtuel de sécurité est développé en un langage de programmation tel que Java, afin de le rendre indépendant du système d'exploitation sous-jacent. En effet, ainsi développé, le serveur virtuel de sécurité devient à même de fonctionner sur n'importe quel type de système d'exploitation à condition qu'une machine virtuelle Java soit insérée entre ce système d'exploitation et ce serveur.

5

10

15

20

- émission de requêtes de service par ladite application logicielle à destination d'un serveur virtuel de sécurité,
- choix, par ledit serveur virtuel de sécurité, d'un serveur de sécurité destinataire, à même de fournir le service de sécurité correspondant à ladite requête de service,
- émission d'informations à destination dudit serveur de sécurité destinataire afin qu'il puisse fournir ledit service de sécurité, certaines au moins de ces informations étant contenues dans ladite requête de service.

Revendications

1. Serveur virtuel de sécurité permettant à un ensemble d'applications logicielles (A_1, A_2, A_3) d'accéder à un ensemble de services de sécurité, caractérisé en ce qu'il possède :
 - des moyens pour recevoir de la part desdites applications logicielles des requêtes de services,
 - des moyens de communication avec des serveurs de sécurité (S_1, S_2, S_3) mettant en oeuvre lesdits services de sécurité,
 - des moyens pour choisir au moins un serveur de sécurité destinataire pour chaque requête de service reçue et pour lui transmettre, via lesdits moyens de communication, des informations lui permettant de fournir le service de sécurité correspondant à ladite requête de service, certaines au moins de ces informations étant contenues dans ladite requête de service.
2. Système selon la revendication précédente, dans lequel lesdites applications logicielles peuvent accéder audit serveur virtuel au travers d'une interface de programmation ou API.
3. Système selon l'une des revendications précédentes, dans lequel ledit serveur virtuel de sécurité est développé en un langage de programmation tel Java.
4. Procédé pour permettre à une application logicielle d'accéder à un service de sécurité, caractérisé en ce qu'il comporte des étapes de :
 1. émission de requêtes de service par ladite application logicielle à destination d'un serveur virtuel de sécurité,
 2. choix, par ledit serveur virtuel de sécurité, d'un serveur de sécurité destinataire, à même de fournir le service de sécurité correspondant à ladite requête de service,
 3. émission d'informations à destination dudit serveur de sécurité destinataire afin qu'il puisse fournir ledit service de sécurité, certaines au moins de ces informations étant contenues dans ladite requête de service.

25

30

35

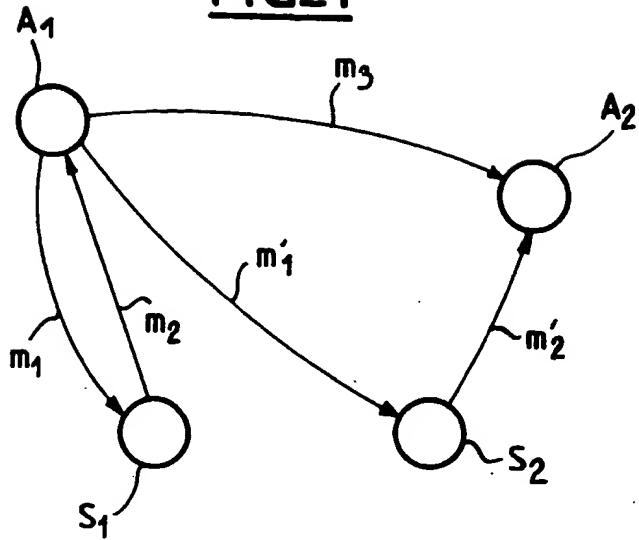
40

45

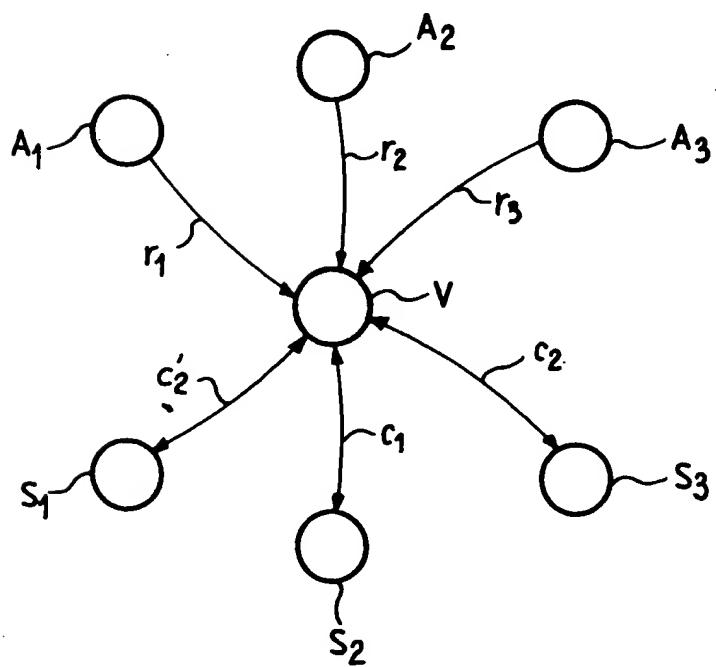
50

55

FIG_1



FIG_2





Office européen
des brevets

RAPPORT DE RECHERCHE EUROPEENNE

Numéro de la demande
EP 00 40 1161

DOCUMENTS CONSIDERES COMME PERTINENTS			
Catégorie	Citation du document avec indication, en cas de besoin, des parties pertinentes	Revendication concernée	CLASSEMENT DE LA DEMANDE (Int.Cl.7)
X	US 5 841 970 A (TABUKI TAKAAKI) 24 novembre 1998 (1998-11-24) * abrégé; figures 2,5,6 * * colonne 3, ligne 57 - colonne 4, ligne 47 * * revendication 1 *	1, 4	H04L29/06 G06F1/00
Y	-----	2, 3	
X	EP 0 817 444 A (SUN MICROSYSTEMS INC) 7 janvier 1998 (1998-01-07) * abrégé; figures 3,4 * * colonne 2, ligne 20 - colonne 3, ligne 24 * * colonne 7, ligne 30 - ligne 38 * * colonne 9, ligne 41 - ligne 52 *	1, 4	
Y	EP 0 677 943 A (IBM) 18 octobre 1995 (1995-10-18) * abrégé; figure 1 * * colonne 1, ligne 1 - ligne 9 * * colonne 4, ligne 21 - ligne 46 * * colonne 5, ligne 26 - ligne 29 *	2	DOMAINE TECHNIQUE RECHERCHES (Int.Cl.7)
Y	BRACKENBURY I F ET AL: "IBM'S ENTERPRISE SERVER FOR JAVA", IBM SYSTEMS JOURNAL, US, IBM CORP. ARMONK, NEW YORK, VOL. 37, NR. 3, PAGE(S) 323-335 XP000783105 ISSN: 0018-8670 * the whole document *	3	G06F H04L
Le présent rapport a été établi pour toutes les revendications			
Lieu de la recherche	Date d'achèvement de la recherche	Examinateur	
LA HAYE	21 août 2000	Sigolo, A	
CATEGORIE DES DOCUMENTS CITES		T : théorie ou principe à la base de l'invention E : document de brevet antérieur, mais publié à la date de dépôt ou après cette date D : cité dans la demande L : cité pour d'autres raisons & : membre de la même famille, document correspondant	
X : particulièrement pertinent à lui seul Y : particulièrement pertinent en combinaison avec un autre document de la même catégorie A : antécédent technologique O : divulgarion non écrite P : document intercalaire		&	

ANNEXE AU RAPPORT DE RECHERCHE EUROPEENNE
RELATIF A LA DEMANDE DE BREVET EUROPEEN NO.

EP 00 40 1161

La présente annexe indique les membres de la famille de brevets relatifs aux documents brevets cités dans le rapport de recherche européenne visé ci-dessus.

Lesdits membres sont contenus au fichier informatique de l'Office européen des brevets à la date du.
Les renseignements fournis sont donnés à titre indicatif et n'engagent pas la responsabilité de l'Office européen des brevets.

21-08-2000

Document brevet cité au rapport de recherche		Date de publication	Membre(s) de la famille de brevet(s)		Date de publication
US 5841970	A	24-11-1998	JP	9081518 A	28-03-1997
			SG	65643 A	22-06-1999
			EP	0762261 A	12-03-1997
			JP	9081519 A	28-03-1997
			JP	9081520 A	28-03-1997
			US	5706427 A	06-01-1998
EP 0817444	A	07-01-1998	JP	10126445 A	15-05-1998
EP 0677943	A	18-10-1995	GB	2288477 A	18-10-1995
			JP	7281974 A	27-10-1995
			US	5687373 A	11-11-1997

EPO FORM P0460

Pour tout renseignement concernant cette annexe : voir Journal Officiel de l'Office européen des brevets, No.12/82